



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of

EVARD et al.

Atty. Ref.: 550-619; Confirmation No. 4576

Appl. No. 10/527,812

TC/A.U. 2183

Filed: June 14, 2005

Examiner: K. Vicary

For: PROCESSING ACTIVITY MASKING IN A DATA PROCESSING SYSTEM

\* \* \* \* \*

December 29, 2009

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

**REQUEST FOR RECONSIDERATION**

Appellants respectfully request reconsideration of the Decision of the Board of Patent Appeals and Interferences mailed November 12, 2009 in the above-identified application. Upon review, Appellants have confirmed to the undersigned that the Board has simply missed the ordinary meaning of the terms clearly set out in Appellants' claim, especially when those terms are well known to those of ordinary skill in the art. The Board's Decision uses generalities to describe the teachings of the cited Qiu reference and again to paraphrase Appellants' claim, but appears to ignore the specific language actually used in Appellants' independent claims. It is the ignored specific language which clearly distinguishes over the prior art. This distinction was explained during the Oral Hearing and the Board members indicated that it was understood at the time. However, apparently subsequent thereto, the Board deviated from the facts set out in Appellants' specification and claims in order to reach its decision.

Appellants will address each of the errors in the Board's Decision in terms of "Appellants' Invention," the "Examiner's Findings," the Board's discussion of the "Issue," the Board's "Findings of Fact" and the Board's detailed "Analysis" below.

**1. The Board errs in describing "Appellants' Invention"**

On page 2 of the Decision, the Board states that "[u]pon determining that the instruction result, when written, will not cause a change, the processor core processes the conditional instruction and subsequently stores the results thereof in a trash register . . . ." This statement by the Board purporting to describe the invention evidences a misunderstanding of the claimed invention.

Firstly, the board's language does not correspond to what is clearly stated in Appellants' independent claim 1. The claim refers to the situation in which the "instruction will or will not be permitted to write data to effect a change in state of said processor core" (claim 1). There is no suggestion in Appellants' claim 1 that "the instruction result, when written, will not cause a change." Should the Board believe this to be included in the claim, the Board is respectfully requested to identify that portion of claim 1 which supports its description of "Appellants' Invention."

Secondly, it is noted that, while the Board cites page 2, lines 1-4 of Appellants' specification as support for its conclusion, lines 3 and 4 actually state that "when the conditional write data processing operation meets its non-write conditions and a write would not otherwise occur." This statement provides no support for the Board's conclusion.

Thirdly, the Board's statement of Appellants' invention suggests that the processor core processes the conditional instruction and "upon determining that the instruction result, when

written, will not cause a change” then takes some action (emphasis added). A logical reading of this statement suggests that, upon determining that the instruction result will cause a change, something different happens. Again, this is not the invention claimed in claim 1 because it specifies “at least one data processing instruction executed by said processor core is a conditional-write data processing instruction” (emphasis added). The claim language specifically states that the “at least one data processing instruction” is always “executed by said processor core.”

How the Board concludes that sometimes this instruction is executed by the processor core and other times “upon determining that the instruction result, when written, will not cause a change,” it is somehow not executed by the processor core, is not understood and is clearly the opposite of Appellants’ claim language.

As purported support for its position, the Decision cites Appellants’ specification, page 7, line 25 through page 8, line 1. However, this portion of the specification clearly indicates that the processor core always processes the conditional instruction thereby confirming the actual claim language. The only question is whether the result is written to a trash register or the destination specified in the instruction itself.

In view of the above three errors, the Board’s Decision evidences that, at best, the Board misunderstood the claim. Appellants concern is that the Board may be attempting to describe Appellants’ invention in generalities broad enough to encompass the cited prior art reference and ignoring the actual language of the claims. As will be seen, the Board’s Decision ignores a critical part of Appellants’ claim, i.e., the data processing instruction is a “conditional-write data processing instruction **encoding condition codes . . .**” which are specifically set out in claim 1.

Nowhere is this portion of Appellants' independent claim 1 disclosed or addressed in the Board's description of Appellants' invention.

It is submitted that the Board has committed reversible error in failing to acknowledge the key portion of the Appellants' invention which distinguishes it from the cited prior art reference.

## **2. The Board may have erred in its statement of the "Examiner's Findings"**

In reviewing the paragraph bridging pages 4 and 5 of the Decision, the Board cites the Examiner's Answer, pages 12-17 (the sentence bridging pages 4 and 5 of the Decision) as support for its conclusion. Appellants have reviewed pages 12-17 and cannot find support for this statement by the Board. However, even if supported by the Examiner, Appellants would note that the Board's recitation of incorrect Examiner findings does not make those findings correct. It will be readily appreciated by those having even ordinary skill in the art that this conclusion as to the Examiner's findings is simply not supported.

Firstly, Appellants' claim 1 states that the result data value will be written to the trash register "upon execution of said conditional-write data processing instruction **when said condition codes within said conditional-write data processing instruction** do not permit a write to effect a change in state of said processor core." (Claim 1 in the paragraph beginning "a trash register"). The reference to "said condition codes" is defined in the context of the previously recited "conditional-write data processing instruction encoding condition codes" also clearly recited in the previous paragraph of claim 1.

The above distinction is central to Appellants' argument since the Qiu reference does not disclose a "conditional-write data processing instruction **encoding** condition codes specifying

conditions . . . .” (emphasis added). Thus, to the extent the Examiner’s statements in the Answer support the Board’s “Examiner’s Findings,” it is clear that the Examiner (and now the Board) have completely missed the central point of Appellants’ claims, i.e., the condition codes which are **encoded** in the “conditional-write data processing instruction.”

As a minimum, for the purpose of appeal, it is specifically requested that the Board cite the portions of the purported “Examiner’s Findings” with specificity especially with respect to the above noted “encoded” limitation, rather than merely reciting six pages of the Examiner’s Answer.

### **3. The Decision errs in its discussion of the “ISSUE” in the present case**

Quite understandably, if the Board has ignored Appellants’ actual claim language and cannot properly identify Appellants’ invention, it will err in stating what issue is before the Board.

The Board notes that the issue is whether Qiu teaches the “claimed invention.” However, rather than resorting to the language of Appellants’ claim to determine what is the “claimed invention,” the Board instead paraphrases Appellants’ claim language. In its paraphrase, the Board misses one critically important portion of Appellants’ claimed invention, i.e., at least one of the instructions executed by the processor core “is a conditional-write data processing instruction encoding condition codes.”

Instead of using the claim language, the Board merely states “when condition codes **associated therewith** do not permit . . . .” (emphasis added). Appellants’ claim is not so broad and at no point does Appellants’ claim suggest that the condition codes are only “associated therewith.” Instead, Appellants’ claim language, quoted above, will show that it is required that

the condition codes are “**encoded within the conditional-write data processing instruction**” rather than merely “associated therewith.”

Because the Board has incorrectly stated “associated therewith” rather than encoded therein, the Board has improperly framed the issue for review. Whether or not Qiu suggests that condition codes are associated with an instruction is not relevant to the issue before the Board. The issues before the Board are (1) whether the Qiu reference contains any teaching or suggestion of the required “conditional-write data processing instruction encoding condition codes” as required by claim 1, and (2) whether those encoded condition codes specify “conditions under which said conditional-write data processing instruction will or will not be permitted to write data to effect a change in state of said processor core.”

It is respectfully requested that the Board identify its rationale for ignoring Appellants’ claimed requirement of “encoding condition codes” and substituting its own conclusion as to the issue, i.e., that condition codes are “associated therewith.”

#### **4. The Board errs in its statements of the “Findings of Fact”**

In its description, the Board describes Qiu in generic terms so broadly as to encompass all possible applications of superfluous operations. This description is a broad concept encompassing “unnecessary multiplication operation,” storing “in a dummy memory location or in a data processing register” and other purported “conditional processes.” While these broad descriptive terms may well describe the Qiu reference, there is no Finding of Fact suggesting that Qiu teaches any encoding “condition codes specifying conditions under which said conditional-write data processing instruction will or will not be permitted to write data to effect a change in state of said processor core.” If the Board agrees that this is not disclosed or suggested in Qiu

such a finding of fact should be stated. If the Board believes that this is disclosed or suggested, the disclosure in the Qiu reference that is the basis for this finding of fact should be cited.

Since it is the Examiner's (and the Board's) contention that Qiu teaches Appellants' claim 1, the Board is respectfully requested to identify as a Fact Finding exactly where Qiu teaches (1) a "conditional write data processing instruction **encoding condition codes**" and (2) "condition codes **specifying conditions** under which said conditional-write data processing instruction will or will not be permitted to write data to effect a change in state of said processor core."

If the Board can find any support in Qiu for either of these two requirements of Appellants' independent claim 1, Appellants will be more able to understand and appreciate the Board's rationale in its Decision. Without such support, the Board's Fact Findings in its Decision is completely unsupported by the Qiu reference.

Moreover, the Board's statement in Finding of Fact 3 that multiplication is "likely to occur" or "not likely to occur" depending on the value bit being "1" or "0" is completely unsupported by the record in this Appeal. One of ordinary skill in the art reading this portion of the Board's Decision may question the Board's understanding of how a data processing apparatus works since, as described in Qiu's column 3, lines 47-67 (as cited by the Board), the value bit positively determines whether the multiplication does or does not occur. There is no suggestion of any "likely" or "not likely" – it either does or does not occur.

Finally, in paragraphs 3 and 4, the Board correctly notes that the Qiu reference, based upon the value key bit, either stores the emulated multiplication in data processing memory location 512 or stores it in a dummy register 516. However, the Board does not admit that this is contrary to Appellants' claimed instruction "encoding condition codes." It is noted that the

decision point - whether to change state or merely store the result of the emulated multiplication in a dummy register - is part of the **algorithm created by the data processing programmer.**

Appellants' claim 1 shifts the security considerations to being an inherent part of the data processing **instructions** (i.e., the conditional-write data processing instruction encoding condition codes) which will be executed by the processor core and thus security of the system is not dependent on programmer implementation.

#### **5. The Board errs in its "Analysis" as to what is required by claim 1**

Consistent with its previous failures to address Appellants' actual claim 1 language, the Board in its Decision suggests that "[i]ndependent claim 1 requires . . ." generalities which are disclosed in the Qiu reference and ignores the specifically claimed features in Appellants' independent claim 1.

Specifically, the Board suggests that execution of a "conditional-write data processing instruction when condition codes associated therewith" do not permit a write to effect a change in the state of a processor core (Decision, page 7, first sentence under "Analysis"). Again, this is the Board's rewriting of claim 1 to change "encoding condition codes" as recited in the claim to the Board's more general language "condition codes associated therewith." This is absolutely wrong and confirms the error in the Board's decision to ignore the central feature of Appellants' claims, i.e., "a conditional-write data processing instruction encoding condition codes."

The above Board error in ignoring Appellants' claim language carries through the remainder of its "Anticipation" analysis and "Obviousness" analysis in the Decision. For example, in the detailed discussion of the definition of "conditional write data processing instruction" and "condition codes," the Board ignores the claim requirement of "encoding" the



condition codes in a conditional-write data processing instruction. While Appellants agree with the Board's obligation to apply the "broadest reasonable meaning" to the words in the claims, the Board provides no evidence in its Decision that it considered the definition of "encoding" or how or in what manner this term modifies "condition codes" in the actual language of Appellants' claim 1. Accordingly, the Board has clearly erred in its analysis of independent claims 1 and 6.

On page 10, the Decision states that the Board agrees with the Examiner that "Qiu's disclosure teaches the disputed limitations, as construed above." Nowhere in the Board's "Analysis" is there any reference to the claim 1 language that the conditional-write data processing instruction actually encodes "condition codes." This error is presumably based upon the Board's failure to properly construe claim 1 as noted above.

The Board further decides that it finds "no basis in the language of the claims before us to substantiate the distinctions that Appellants are seeking to establish." There is no requirement that a claim recite the benefit of the claimed combination. However, if the claimed combination inherently provides a benefit missing from the prior art, that benefit can distinguish the prior art.

Appellant merely pointed out that Qiu teaches a solution to the simple power analysis (SPA) problem whereas the claimed invention is a solution to both the SPA and to differential power analysis (DPA) problems. While Appellants completely agree that there is no recitation of SPA or DPA in the claims, it is noted that Appellants never argued that this was in the claim.

What Appellants did argue in its Appeal Brief and at the Oral Hearing is that Qiu's disclosure can only solve the SPA problem and does not defeat DPA, as does the present invention. Appellants clearly pointed out, and at least during the Oral Hearing the Board members appeared to understand, that defeating differential power analysis is a consequence of Appellants' claim limitations, i.e., conditional-write data processing instruction encoding

condition codes. Of course, the un-claimed benefit of the claimed combination of elements in Appellants claims can distinguish the cited prior art.

The Board's attention is directed to the transcript of the November 4, 2009 Oral Hearing which has recently been forwarded to the Appellants (mailed on December 8, 2009, after the Board's Decision was mailed on November 12). Appellants' counsel pointed out on transcript page 7, lines 15-18, that the Qiu reference is trying to do dummy operations as well "but when it says do the dummy operation, it gives a signature of that decision." Counsel then pointed out that "Because it's not encoded within a conditional write instruction. It's part of the algorithm. So that's the difference. The -- ours is not an algorithm based systems. It's a write instruction and hidden in the write instruction, encoded within the instruction, as the claim says --." APJ Homere further stated that "I don't understand why this would not be instructions that are conditional -- as a matter of fact, QIU refers to them as conditional processes, okay, in the section, in the section that I just pointed you -- directed you to." Counsel responded by noting that

"... the operative language is ... a conditional write data processing instruction encoding condition codes specifying conditions under which blah, blah, blah. It will or will not be permitted to write data to effect a change in state.

So QIU doesn't have any conditional write instruction. It doesn't have any instruction that has an encoded condition code ..."

(Transcript, page 8, lines 16-22).

Appellants' counsel noted that the problem with the Qiu reference is that someone attempting to defeat the Qiu system will throw a smart card

"into an analyzer, and they put signal inputs into it. They look at then the output. What happens? And so by putting in a whole sequence of different signals, timing, power levels and all of that,

they will get different outputs. By doing that repeatedly, that's the differential power analysis, even if QIU is built into your smart card system, they will ultimately see the fingerprint of the branching that occurs in the algorithm that's used to protect the smart card, and they will then be able to deduce what your key is and use that card and get money out of your ATM."

(Transcript, page 12, lines 1-9).

In response, Judge Homere stated that "that's the exact problem that QIU is trying to resolve" to which Appellants' counsel completely agreed (Transcript, page 12, lines 13-15) that both the present invention and the Qiu reference are trying to protect a smart card. However, counsel pointed out to the Board that "[b]oth systems are trying to protect that smart card. QIU protects against the simple power analysis [SPA]." (Page 12, lines 17-18 of the Transcript).

However, the deficiency in the Qiu teaching is discussed by counsel beginning on page 12, line 23 carrying over to page 13, line 1. Counsel then explained "[a]nd in our invention, we don't do that. We don't have that branching determination that is made, so you can't see it. It's encoded in the instruction, in these conditional-write data processing instructions, and that's the trick. That's why this thing is -- both of them defeat power analysis. QIU only defeats the simple power analysis [SPA]. Ours defeats both the simple power analysis and the more advanced differential power analysis . . . ." (Transcript, page 13, lines 1-7). Because Judge Homere did not question any of the distinctions raised between the Qiu analysis and the claim 1 analysis, counsel concluded that Judge Homere understood the difference.

However, Judge Homere subsequently asked "What language here in this claim that captures the concept of a differential power analysis here?" (Transcript, page 13, lines 13-14). Counsel for Appellants responded by pointing out that "The language that enables differential power analysis to be defeated is the language up in the third paragraph [of claim 1] that says at

least one data processing instruction executed through the -- is a **conditional-write data processing instruction encoding condition codes**, specifying conditions under which conditional-write data processing will or will not be permitted to write data to effect a change.” (emphasis added, Transcript, page 13, lines 20-25). In response, APJ Homere stated “Okay, I think we understand each other.” (Transcript, page 14, line 1).

At this point in the Oral Hearing, Judge Homere rested and Judge Hughes began asking questions. Judge Hughes, as evidenced by the discussion in the Transcript at page 15, lines 10-23, indicated that he was reading the Qiu reference as having instructions and Appellants’ counsel pointed out that “Take the definition of instructions. We attached a copy to the Reply Brief. Examiner never saw it, so take it for what it’s worth” or suggested “do your own Internet search.” (Transcript, page 15, lines 21-25). Judge Hughes seemed to have understood the distinction when during the Oral Hearing he stated

“And you’re saying QIU does not have instructions that are so encoded?”

MR. SPOONER: Right, exactly, That’s the first thing we’re saying QIU doesn’t have.

JUDGE HUGHES: Okay.

MR. SPOONER: The second thing we’re saying QIU doesn’t have is the trash register as defined in the claim. Not QIU [doesn’t have] a trash register, but he doesn’t have a trash register that has any of the other attributes, interrelationship attributes specified in the claim to which a data -- result data value will be written instead of a data processing register.”

(Transcript, page 16, lines 5-14).

At the above point in the Oral Hearing, it was clear that both Judge Homere (as previously indicated) and Judge Hughes (subsequently asking no further questions ) understood that Appellants’ claim required “conditional-write data processing instruction” which included

encoded “condition codes specifying conditions . . . .” How or why the Board subsequently forgot or ignored this critical claim limitation is not understood. However, in view of the above, it is clear that the Board in its subsequent Decision ignored this feature of Appellants’ claim language, ignored the specific teachings of Qiu, did not demonstrate how or where the Qiu reference taught the specific claim language or the specifically claimed interrelationships and, as a result, reached the wrong conclusions of law.

There is no requirement that an applicant recite the benefits of a claimed invention in the claim. The benefits of Appellants’ claims – being able to defeat DPA – are the logical consequence of Appellants’ claimed elements and their claimed interrelationship and particularly the claimed “conditional-write data processing instruction **encoding condition codes** specifying conditions under which said conditional-write data processing instruction will or will not be permitted to write data to effect a change in state of said processor core.” The independent claims describe Appellants’ invention which is the arranging of an individual instruction such that it encodes condition codes. This arrangement defeats DPA attacks by hiding the operation of the data processing at the level of each individual instruction, rather than within algorithmic branches of program code as is done by Qiu. The characteristic signature of algorithmic branches (as done by the Qiu reference) will defeat simple power analysis (SPA) but will not defeat the more persistent differential power analysis (DPA) which is the additional problem solved by the present invention but ignored by the Qiu patent.

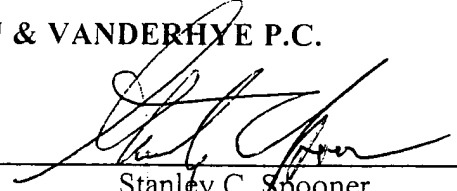
Accordingly, reconsideration of the Board’s Decision regarding the rejection of claims 1-10 under 35 USC §102 and §103 is respectfully requested.

EVRARD et al.  
Appl. No. 10/527,812  
December 29, 2009

Respectfully submitted,

**NIXON & VANDERHYE P.C.**

By: \_\_\_\_\_

  
Stanley C. Spooner  
Reg. No. 27,393

SCS:kmm  
901 North Glebe Road, 11th Floor  
Arlington, VA 22203-1808  
Telephone: (703) 816-4000  
Facsimile: (703) 816-4100